23.3 A Low-Power True Random Number Generator using Random Telegraph Noise of Single Oxide-Traps

Ralf Brederlow[1], Ramesh Prakash[2], Christian Paulus[3], Roland Thewes[1]

[1]Infineon Munich, Germany,
[2]now with Agere Systems, San Jose, CA
[3]now with Siemens, Munich, Germany

Secure encryption depends on the quality of random numbers available for generating encryption keys. The highest level of security is only guaranteed when true random numbers are used [1, 2]. Therefore, such circuits are necessary building blocks in state-of-the-art security controllers. A true random number generator (TRNG) is presented that utilizes the noise produced by single-oxide traps in small area MOSFETs in combination with built-in redundancy. The new concept enables low power and area consumption, is robust against environmental noise and supply voltage variations, and is thus suitable for operation within security controllers.

In integrated circuits, device noise is the only available source of true randomness. The most frequently used concept is to amplify the white thermal noise of a resistor [3-5], to supply it to the voltage control input of a voltage controlled oscillator, and to finally sample the resulting jitter. However, problems arise with additional non-white amplifier noise and with offsets [4-6]. Other approaches use silicon nano-devices [7] or MOS diodes after soft-breakdown [8] as random sources. These have higher noise levels than thermal noise, making the final circuit more robust. However, the noise is colored and the circuits fail certain tests for randomness.

Figure 23.3.1 shows the low frequency noise of 0.12µm MOS transistors with minimum device area. Their noise spectra are white up to a corner frequency. Above this frequency the noise power decreases with $1/f^2$. Below this frequency the noise voltage is much higher compared to thermal noise. This is typical for a single trap related noise spectrum [9] and corresponds to the time domain characteristic as shown in the upper left part of Fig. 23.3.2. The figure also shows the concept of the TRNG introduced here: the noise is amplified and compared with a reference voltage using a clocked comparator. The resulting data are shown below the graph in Fig. 23.3.2. Since usually the average durations of higher and lower voltage levels are not equal, the output data are usually biased, i.e. the probability of a logical '1' is not equal to the probability of a logical '0'. As we will see later, this statistical bias causes the unprocessed data to fail some tests for randomness. This problem can be solved by applying the von Neumann algorithm (see upper right part of Fig. 23.3.2) to the output data.

Figure 23.3.1 also illustrates the statistics of oxide trap noise for small devices. By implementing a sufficiently large array of such devices, the availability of a white noise source within the desired frequency band (given by the sampling frequency) is guaranteed. Before using a particular device for random data generation it must be selected from the array. Fig. 23.3.2 also shows a corresponding realization. To find out the best fitting device the decoder selects one device after the other for quality checks (e.g. noise bias). For an embedded TRNG this can be realized by software. After having finished the check for all devices, the best suited device is selected. Redundancy is almost for free. Since the trap noise statistics do not change much over time even with supply voltage or temperature changes, this routine has to be run only once (assuming non-volatile memory is available). However, in most practical cases it is useful to continuously monitor the quality of the random numbers.

Due to the significantly larger signal of the noise source used here as compared to thermal noise, and due to the differential implementation, we are able to avoid power hungry oscillator circuits [4-5] in the noise-to-digital random data conversion.

In the noisy environment of a security controller, a fully differential approach for the analog-noise-to-digital random data conversion is strongly preferable. A schematic of the realized circuit is shown in Fig. 23.3.3. The noise amplifier in the generator block amplifies the noise of a selected pair of small area MOSFETs. The core circuit is a differential stage consisting of transistors T1-T3 and T_{i1}-T_{i2} (with index i for the currently selected array transistor pair). Especially for the small area input devices, good matching cannot be guaranteed. For high DC-gain, offsets would be amplified and could even disrupt DC-biasing conditions. Therefore, to reduce the gain for DC and frequencies below ~5kHz, a passive low pass filter is implemented for the load transistor (T1, T2) biasing. Above the corner frequency of the filter the circuit amplifies the noise of the input devices by a factor of ~50. High-pass filtering (Fig. 23.3.3), before applying the signals to the input of the comparator, removes the remaining offset and sets a common DC-bias for the comparator inputs. The comparator (Fig. 23.3.3) is designed for low input offset and optimized for small memory effects. Since only matching of both filter branches matters and not the absolute corner frequency, we do not need to accurately determine the absolute value of the resistors for the filters and can thus use MOSFETs biased in the sub-threshold regime to save area (see lower left of Fig. 23.3.3).

In Fig. 23.3.4, a digital output stream of the difference signal between the two comparator outputs is shown. The data seem to be almost random. However, longer runs of several sequential 0's or 1's are obvious especially for the data sampled at 5MHz. This is explained by the fact, that the trap switching frequency is low compared to the sampling frequency, so that trap states are sampled several times without having changed. Applying the v. Neumann algorithm to the data removes these long runs and statistical biasing of the random data. However, the data rate in Fig. 23.3.5 is reduced by a factor of 4 to 8 depending on device and sampling frequency (for ideal white noise input data it is reduced by a factor of four). This is not an issue, for most applications, since much lower data rates are sufficient.

Figures 23.3.5 and 23.3.6 show the results of mathematical tests using the tests described in [10] for a number of different transistor pairs within one chip, both before and after application of the von Neumann correction. While due to statistical biasing and long runs the raw data sometimes fail the security tests, all devices clearly fulfill the mathematical tests after the correction. Common χ^2- and serial correlation-tests are also fulfilled (not shown here). Due to the redundancy in the noise sources, the yield of high quality noise sources is high. The circuit is fully functional for supply voltages from 1.2V to 1.7V, even if operated with supply voltage ripples and substrate cross-talk signals of up to 300mV. This is in good agreement with the simulated power supply rejection ratio of 50dB.

The circuit consumes 20µW of DC-power and additional 30µW/MHz of clocked power depending on sampling frequency, corresponding to a total power consumption of 50µW at 200kb/s random output data. This compares to 2.3mW at 10MHz [5], or 3.9mW at 1MHz [4] data rate for alternative approaches [4-5].

The circuit is fabricated in a 0.12µm digital CMOS technology using standard devices only, and has an area of 9000µm² (Fig. 23.3.7).

References:

[1] FIPS 140-2, "Security Requirements for Cryptographic Modules," *National Institute of Standards and Technology*, GPO, Washington DC, 1999.
[2] W. Killmann, W. Schindler, "Functional Classes and Evaluation Methodology for True Random Number Generators," http://www.bsi.de/zertifiz/zert/interpr/trngk31e.pdf, 2002.
[3] B. Jun, P. Kocher, "The Intel Random Number Generator," white paper, http://www.cryptography.com/resources/whitepapers/IntelRNG.pdf, 1999.
[4] C. S. Petry, J. A. Connelly, "A Noise Based IC Random Number Generator for Applications in Cryptography," *IEEE Trans.Circuit & Systems*, vol. 47, no. 5, pp. 615-621, May, 2000.
[5] M. Bucci, et al., "A High Speed Oscillator Based True Random Number Generator for Cryptographic Applications on a Smart Card IC," *IEEE Trans. Computers*, vol. 52, no. 4, pp. 403-409, April, 2003.
[6] D. J. Kinnimet, E.G. Chester, "Design of an On-Chip Random Number Generator Using Metastability," *Proc. European Solid-Sate Circuit Conf.*, pp. 595-598, Sept., 2002.
[7] S. Fujita, et al., " Si Nanodevices for Random Number Generator Circuits for Cryptographic Security," *ISSCC Dig. Tech. Papers*, pp. 294-295, Feb., 2004.
[8] S. Yasuda, et al., "Physical Random Number Generator Based on MOS structure after soft breakdown," *IEEE J. Solid-State Circuits*, vol. 39, no. 8, pp. 1375-1377, Aug., 2004.
[9] G. Wirth, et al., "Modelling of Statistical Low-Frequency Noise of Deep-Sub Micrometer MOSFETs," *Trans. on El. Dev.*, vol. 52, no. 7, pp. 1376-1388, July, 2005.
[10] J. Walker, 'ENT — Entropy calculation and analysis of putative random sequences," http://www.fourmilab.ch/random/, 1997.

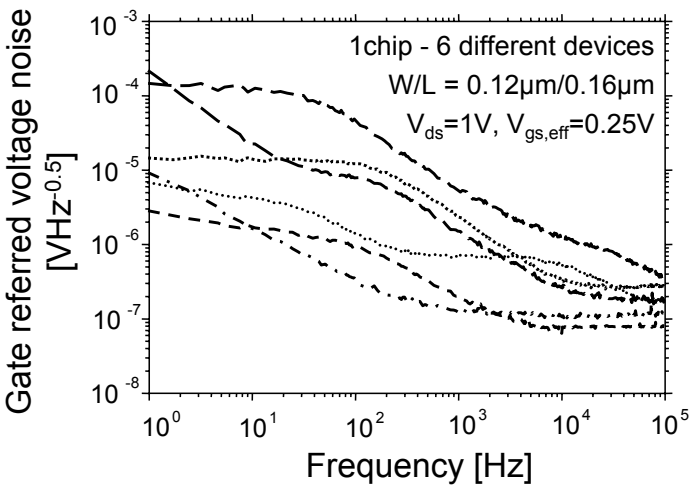

Figure 23.3.1: Noise spectra of several small area MOSFETs.

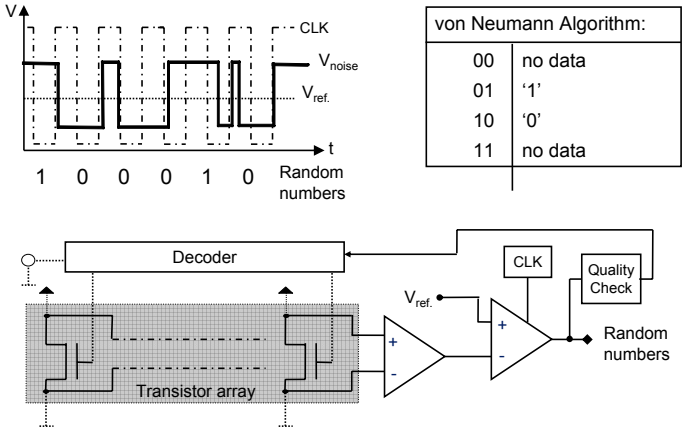

Figure 23.3.2: Schematic illustration of the TRNG principle.

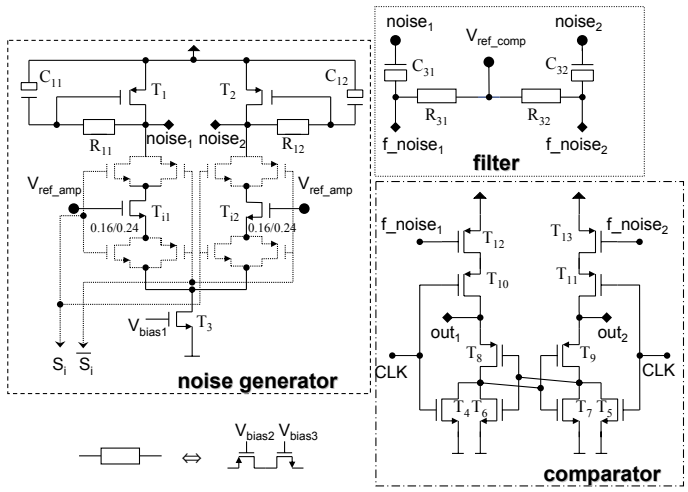

Figure 23.3.3: Schematics of noise generator, filter, and comparator circuit. For simplicity, transistors T_{i1} and T_{i2} represent the whole array of selectable transistors.

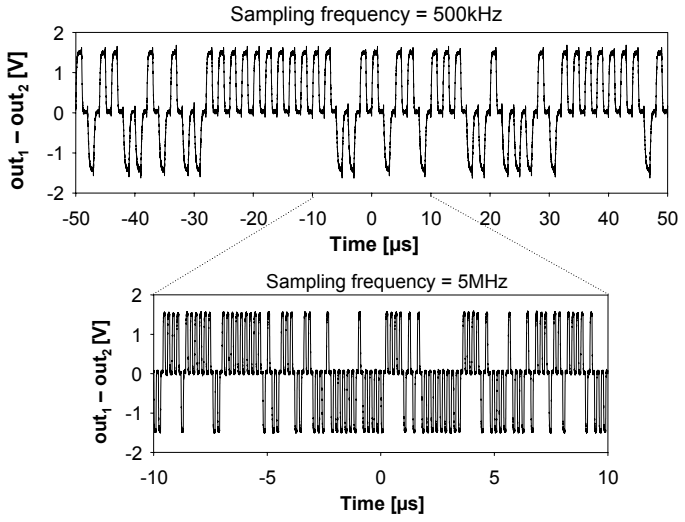

Figure 23.3.4: Measured raw output waveforms for two sampling frequencies (taken at different times).

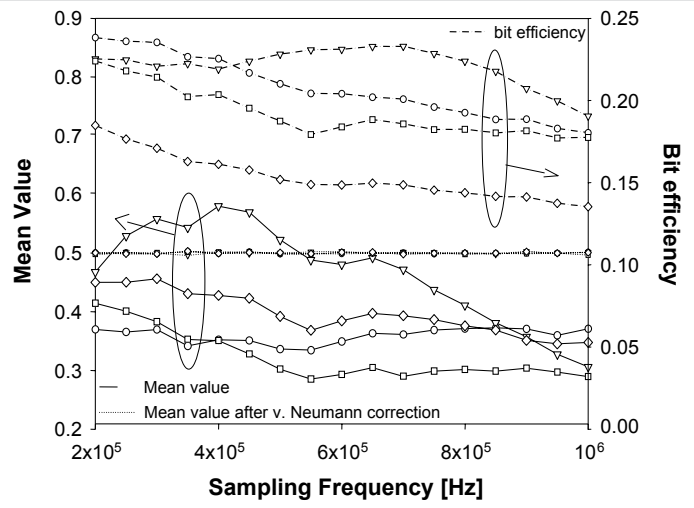

Figure 23.3.5: Random data mean values (100k samples) versus sampling frequency for typical noise sources in a typical circuit before and after v. Neumann algorithm, and bit efficiency when using the algorithm.

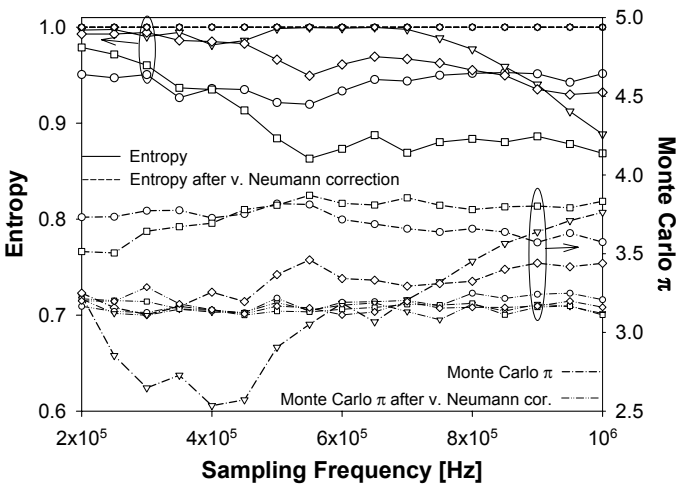

Figure 23.3.6: Random number (100k samples) quality plots for typical noise sources in a typical circuit: entropy (left) and Monte Carlo π (right) before and after v. Neumann algorithm.

Continued on Page 663

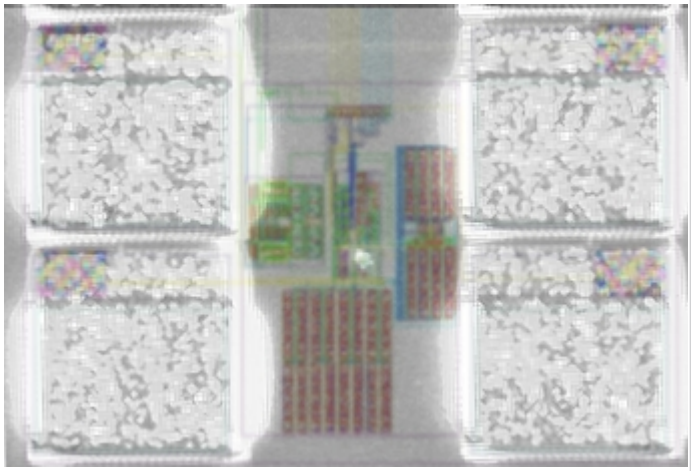

Figure 23.3.7: Chip micrograph of the implemented true random number generator in a 0.12µm standard CMOS technology.

